Anjelica Dortch

Senior Director U.S. Government Affairs
&
Head of Global Cybersecurity Policy

SAP America, Inc.

Written statement prepared
for the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Hearing entitled,

“Growing the National Cybersecurity Talent Pipeline”

June 22, 2023

Chairman Garbarino, Ranking Member Swalwell, and members of the subcommittee on Cybersecurity and Infrastructure Protection, thank you for the opportunity to appear before you today to discuss the importance of growing our nations cybersecurity talent pipeline. My name is Anjelica Dortch, and I am the Senior Director of U.S. Government Affairs and Head of Global Cybersecurity Policy for SAP – the world's largest enterprise software application provider.

On behalf of SAP, I commend this subcommittee for working together to highlight innovative approaches that address the longstanding challenges we face as a nation in developing, attracting, and retaining cybersecurity professionals. My testimony will address the role SAP plays in creating opportunities for current and future cybersecurity professionals and our commitment to help close the cybersecurity skills gap.

I would first like to provide the subcommittee with a brief overview of my professional background. Prior to joining SAP, I led scale up of tech policy positions at IBM within the Government and Regulatory Affairs team with a focus on artificial intelligence, hybrid cloud, and intellectual property. I spent 10 years working for a variety of U.S. federal agencies including the Executive Office of the President as a Senior Technology Advisor where I led coordination of several cybersecurity workforce initiatives to include leading the first-ever government-wide tech and cyber hiring event and the federal cybersecurity reskilling academy. Additionally, I contributed to the development of U.S. policies and strategies including the 2018 National Cybersecurity Strategy, the Presidential Executive Order on America's Cybersecurity Workforce, the U.S. Federal Cloud Computing Strategy (or Cloud Smart), and the Administration's Report on Artificial Intelligence. Lastly, I'm passionate about getting individuals who look like me into the cybersecurity field.

About SAP

SAP is a globally recognized technology leader helping organizations of all sizes and in all sectors run at their best. Our customers generate 87% of total global commerce ($46 trillion). Additionally, 99 out of the 100 largest companies in the world are SAP customers. We operate in over 150 countries and have over 100,000 team members worldwide. From manufacturing and distribution of vaccines to modernizing the U.S. Department of Defense travel management system, SAP's core purpose is to help the world run better and improve people's lives. I believe SAP is uniquely suited to provide the subcommittee with insights today into the opportunities and challenges we face in addressing critical shortages in America's cybersecurity talent pipeline.

Our Achievements

For over 50 years, SAP has worked to foster trust through responsible actions in the context of security, privacy, compliance, and transparency. To achieve this, we rely on talented cyber and national security professionals from around the world. I'd like to highlight two organizations at SAP that play a critical role in (1) strengthening the security of SAP and our customers and (2) ensuring we fulfill national security requirements and comply with critical infrastructure regulations.

Our SAP Global Security team (or SGS) is responsible for product and application security, cyber defense and design, security risk and compliance, physical security, and most of all trust. Through the leadership of our SAP Chief Security Officer, Mr. Timothy McKnight, we have made significant inroads in attracting, retaining, and growing a diverse and high performing global security team. As of 2023, the SAP Global Security team has surpassed the national average of women working in cybersecurity, and it has more than doubled the number of women in cybersecurity management roles. The Office of the Chief Trust Officer within our security organization has reached 50/50 gender parity. Furthermore, the generational diversity of the SAP Global Security team is drastically different than that of the U.S. federal government. Over 60 percent of the organization is comprised of Millennial and Gen Z cybersecurity professionals. Meanwhile, only 4 percent of technology

professionals in the U.S. federal government are under the age of 30. As you can see, the SAP Global Security Team is committed to providing equal opportunities and ensuring that everyone has a chance to develop and grow in the cybersecurity space.

For SAP to serve government customers worldwide, we must also work collaboratively with the national security community. Our Government Security and Secrecy team (or GS2) led by Mr. Martin Merz, ensures the fulfilment of national security requirements, and manages cooperation and coordination with all relevant government security authorities. Most of this team is comprised of former national security professionals who spent upwards of 30 years working for the government. In the past 12 months alone, the Government Security and Secrecy team has grown 34 percent by attracting cleared national security professionals to SAP. Close to 40 percent of this team is made up of women, and they are only 7 percent away from reaching 50/50 gender parity for women in management roles.

How are we growing a diverse cybersecurity talent pipeline at SAP?

Early Talent Program

To attract and recruit young or early career cybersecurity professionals, SAP established the Global Security Early Talent Program[1]. This two-year program is designed for high-performing early career professionals, with little to no professional experience, and have a basic understanding of information technology and security topics. All participants start the program with their first rotation at our SAP America headquarters in Newtown Square, Pennsylvania, and spend at least one rotation abroad at our SAP global headquarters in Waldorf, Germany. The six months abroad is fully covered by the Global Security Early Talent Program. After completing the Security Rotational Program, participants move into a new full-time role within the SAP Global Security team that best matches their skills and interests. This model has expanded and diversified our pool of cybersecurity candidates, along with higher retention rates once program participants shift to full-time roles. Additionally, these types of rotational programs provide greater exposure and flexibility for early career cybersecurity professionals to explore different roles or specialties within this field rather than immediately locking them into a distinct role or occupational series.

Autism at Work Program

At SAP, we view neurodiversity as a competitive advantage. That's why in 2013 we launched a groundbreaking Autism at Work program which leverages the unique abilities and perspectives of colleagues on the spectrum to foster inclusion at SAP.[2] We have the longest running Autism at Work program among major companies. The SAP Autism at Work program provides a pathway and support for neurodiverse cybersecurity professionals. We support neurodiverse candidates during the hiring process and offer a variety of resources to facilitate the success of the employee once they are onboarded. Neurodiverse individuals frequently need workplace accommodations, such as headphones to prevent auditory overstimulation in order to activate or maximally leverage their abilities. In many cases the accommodations are manageable, and the returns are great for both the employee and employer. But to realize the benefits, most organizations must adjust their recruitment, selection, and career development policies to reflect a broader definition of talent.

[1] Global Security Early Talen Program at SAP - https://www.sap.com/documents/2022/01/de2934fb-127e-0010-bca6-c68f7e60039b.html

[2] SAP Autism at Work Program - https://www.sap.com/about/careers/your-career/autism-at-work-program

SAP NS2 Serves

The U.S. Department of Veteran Affairs estimates there are over 19 million living veterans in America. To address the growing need to support veterans and their transition into critically needed national security roles, SAP National Security Services (or NS2) – an independent U.S. subsidiary of SAP – established NS2 Serves[3]. The program was founded to empower veterans and ease their integration into civilian life by providing free, skills-based training for today's high-demand, high-tech careers. NS2 Serves provides free training and employment assistance to veterans. The program is available to impending or honorably discharged post-9/11 U.S. military service veterans, who have left service in the last ten years and reservists (including disabled veterans), service members with orders to leave active duty, and Gold Star spouses who meet eligibility requirements. The 8-to-12-week intensive program provides students at all technical levels with world-class software solutions training and certifications for a variety of well-paying careers within U.S. national security and commercial enterprises. NS2 Serves is committed to train and place 600 veterans in new national security careers by 2025. To date, we have trained over 400 veterans and achieved more than a 90% graduation rate. As a result, all graduates of NS2 Serves have gained job offers. This program gives veterans valuable skill sets and a high degree of employability. They can achieve a strong sense of purpose that often averts some of the impacts of Post-Traumatic Stress Disorder (PTSD), homelessness, and other mental health challenges. Many of our veterans want to continue to contribute to their country, and they can do so across our government where SAP technologies are widely used. SAP NS2 is making the investment to provide veterans with that pathway. The next cohort will launch Fall 2023.

Apprenticeships

As a multi-national organization operating in more than 150 countries, SAP views apprenticeships as an integral part of the development, recruitment, and retention of our workforce. At the SAP global headquarters in Waldorf, Germany approximately 25% of our team members joined through an apprenticeship. Last year, the Administration announced the 120-day Cybersecurity Apprenticeship Sprint to increase awareness of current cybersecurity-related registered apprenticeship programs while recruiting employers and industry associates to expand and promote apprenticeships. However, the pathway to establish a U.S. based apprentice program comes with obstacles and challenges that this committee should explore.

An Ambitious Diversity, Equity, and Inclusion (DEI) Strategy

The data is clear, a diverse and inclusive workplace leads to more innovation and allows us to better serve and represent our customers around the globe. At SAP, DEI is part of our DNA. We are intentional about addressing representation gaps within the technology sector to include cybersecurity roles. In 2017, we set a goal of 35% women in our workforce by 2030, and in December 2022, we achieved that goal. Our next goal is to reach 50/50 gender parity globally. We hold ourselves accountable by publishing our progress and specific goals, including increasing the number of women in technical roles to 40% and doubling the number of women and underrepresented minorities in senior roles by 2030. We intentionally work to attract, hire, retain, and develop talented people of diverse backgrounds, points of view and experiences. Our strong commitment to allyship drives a more open, accepting, and inclusive culture, so people can bring their whole selves to work and perform at their best.

[3] NS2 Serves Training & Employing Veteran Program - https://ns2serves.org/

SAP University Alliances

For more than 25 years, SAP has worked to establish relationships with academic institutions across the world through our University Alliances Program. In the U.S., we engage between 125,000 to 150,000 students per year through roughly 400 established partnerships with universities and community colleges. The program includes Minority Serving Institutions (MSIs) to include Morehouse, Spellman, and Fayetteville University. We continue to expand these alliances across the world to create new awareness and enthusiasm for SAP and career opportunities in the cybersecurity field.

An Education Focused Corporate Social Responsibility Strategy

SAP believes that investing in education is investing in the skills and talents of the next generation — the foundation for the future growth and prosperity of our nation. We invest in innovative education models and foster our engagement with multistakeholder partnerships to enable pathways to employment and entrepreneurship in the digital, social, and green economy for youth in need (Under-represented, under-served, and under-privileged youth between the age of 16 to 24). Last year, SAP began supporting the Last Mile Education Fund[4] – a program focused on increasing diversity in tech by addressing critical gaps in financial support for low-income underrepresented students. For example, Sadie, a first-generation college student and a member of the Tohono O'odham tribe, triumphed over the challenges of growing up on a rural reservation where she faced unique challenges due to the limited resources and opportunities. Despite the scarcity of Native Americans in tech, Sadie became one of the first in her village (Pisinmo'o) to earn a cybersecurity degree. Now, she is on her way to becoming a product manager at a leading cybersecurity company, blazing a trail for others in her community. Sadie's journey embodies resilience, determination, and the power to redefine what is possible in the cybersecurity space. More partnerships and investments into innovative programs like the Last Mile Education Fund are needed to help individuals overcome socioeconomic barriers to starting a career in cybersecurity.

International Observations and Trends

Immigration Reforms Outside the United States

With a global footprint spanning over 150 countries, SAP can share international observations and growing trends in workforce development. The global cybersecurity talent shortage has forced some of our allies to explore reforms to their immigration policies for the purposes of removing migration hurdles for high-skilled workers in technology and cybersecurity roles. Canada, Australia, and Germany are currently instituting reforms that amend education, employment, language, and compensation requirements. In some instances, the path to achieving dual citizenship has been lowered to ensure retention of migrants who make significant contributions to the economic prosperity of the country. Some of these reforms include launching a streamlined process powered by user-friendly web-based applications that provide immigration decisions within 30 to 60 days. Overall, the competition for American cybersecurity professionals will continue to increase as allied nations enact "cyber visas" to attract top talent to their regions.

[4] SAP Partners with Last Mile Education Fund - https://news.sap.com/2022/06/last-mile-close-technology-gender-gap/

European Union Cybersecurity Skills Academy

In April, the European Union launched the Cyber Skills Academy[5] which is a European initiative aimed at bringing together existing cybersecurity education programs and improving their coordination, to close the cybersecurity talent gap and boost EU's competitiveness, growth and resilience. The Cyber Skills Academy is built on four pillars. The first pillar addresses education and training to foster EU cybersecurity knowledge. The second pillar will provide information on certification capacity and visibility into funding opportunities. The third pillar includes stakeholder involvement, and the fourth pillar will monitor progress of the initiative. EU member states and industry have been urged to support the development and recognition of micro-credentials, and the EU Commission is tasked with creating a centralized repository for all EU cybersecurity programs, trainings, and certifications via the "Digital Skills and Jobs Platform" by the end of 2023. The success of the EU's efforts to bolster its cybersecurity pipeline will depend on a strong collaboration with industry and EU member states. We encourage the subcommittee to continue monitoring the progress of this national initiative.

Recommendations

With growing demands for cybersecurity talent, Congress has an opportunity to drive impactful reforms that can give Americans multiple pathways into cybersecurity careers. The United States has a tremendous opportunity to engage, employ, and develop a more inclusive and diverse workforce into high-demand, high-paying cybersecurity jobs that can strengthen our national security and economic prosperity. SAP submits the following recommendations and actions for consideration by Congress:

1. Pass the Jumpstart Our Businesses by Supporting Students Act of 2023 (or the JOBS Act), cosponsored by Representatives Bill Johnson, Lisa Blunt Rochester, Michael Turner, and Miki Sherrill. The bill would extend Pell grant eligibility to short-term job training programs for high demand occupations like cybersecurity.

2. Scale and centralize successful job training and employment programs that transition veterans more easily into cyber and national security roles.

3. Identify and highlight best practices for providing neurodiverse Americans a pathway to join the cybersecurity workforce.

4. Shift the U.S. federal government away from "home grown" human capital management solutions and towards trusted and robust commercial solutions that can reduce the time-to-hire and improve the user experience for cybersecurity professionals seeking to join the civil service.

In closing, it has been an honor to appear before this subcommittee today on behalf of SAP. It is my hope that these recommendations, observations, and best practices support the advancement of positive change that leads to a more secure nation. Thank you, Chairman Garbarino, Ranking Member Swalwell, and members of the subcommittee for your dedication to growing our nations cybersecurity talent pipeline. I'll be happy to answer any of your questions.

[5] European Union Cybersecurity Skills Academy - https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

Anjelica Dortch (She/Her)
Senior Director U.S. Government Affairs – Head of Global Cybersecurity Policy
SAP America, Inc.
1399 New York Avenue NW Suite 800
Washington, D.C. 20005
Phone: (240) 205-4208
Email: Anjelica.Dortch@sap.com
Twitter: @AnjelicaDortch
LinkedIn: https://www.linkedin.com/in/anjelicadortch

Anjelica Dortch is Senior Director of U.S. Government Affairs and Head of Global Cybersecurity Policy at SAP America where she manages the company's cybersecurity, artificial intelligence, and workforce policy portfolio. Prior to joining SAP, Ms. Dortch led scale up of tech policy positions at IBM within the Government and Regulatory Affairs team with a focus on artificial intelligence, hybrid cloud, and intellectual property. Ms. Dortch spent 10 years working for a variety of U.S. federal agencies including the Executive Office of the President as a Senior Technology Advisor where she led coordination of several cybersecurity workforce initiatives to include leading the first-ever government-wide tech/cyber hiring event and the federal cybersecurity reskilling academy. She has contributed to the development of U.S. policies and strategies including the 2018 National Cyber Strategy, the Presidential Executive Order on America's Cybersecurity Workforce (EO 13870), the U.S. Federal Cloud Computing Strategy (or Cloud Smart), and the Administration's Report on Artificial Intelligence. Ms. Dortch is the recipient of the Office of Management and Budget Special Achievement award, Women Leading for Impact award, the University of Maryland Outstanding Alumnus award, and Federal Computer Week's Rising Star award. Ms. Dortch is a Bloomington, Indiana native and holds a Bachelor of Arts degree in Philosophy and a Master of Science in Financial Management and Information Systems from the University of Maryland.

SAP Global Communications (May 16, 2023)

SAP: The World's Largest Provider of Enterprise Application Software

Customers

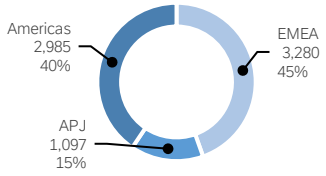
- SAP customers generate 87% of total global commerce ($46 trillion)
- 99 of the 100 largest companies in the world are SAP customers
- 97 of the 100 greenest companies in the world run SAP
- 85 of the 100 largest companies in the world are SAP S/4HANA customers
- Approximately 80% of SAP's customers are SMEs

Financials

Revenue – FY2022, continuing operations, excluding Qualtrics (non-IFRS, growth rates @cc)	
Cloud revenue	€11.43b (+ 23%)
Cloud and software revenue	€25.39b (+ 3%)
Total revenue	€29.52b (+ 4%)
Share of more predictable revenue (total of cloud subs. and support rev. and software support rev.)	79%
Revenue – Q1/2023 continuing operations, excluding Qualtrics (non-IFRS, growth rates @cc)	
Cloud revenue	€3.18b (+22%)
Cloud and software revenue	€6.36b (+ 8%)
Total revenue	€7.44b (+9%)

Revenue by region Q1/2023

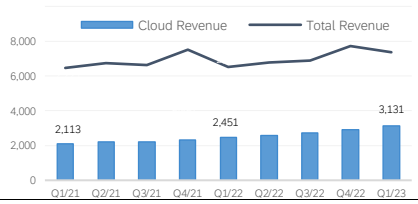
(€ m, continuing operations, non-IFRS at constant currencies / share of total rev. in %)



Outlook 2023 contin. ops., excl. Qualtrics (non-IFRS@cc)	
Cloud revenue	€14.0b to €14.4b, up 23%-26%@cc
Cloud and software rev.	€26.9b to €27.4b, up 6%-8%@cc
Operating profit	€8.6b to 8.9b, up 8%-11%@cc
Share of more predictable revenue	approx. 82%
Free cash flow	approx. €4.9b
Ambition 2025 excl. Qualtrics (non-IFRS), updated 5/16/2023	
Cloud revenue	>€21.5b
Total revenue	>€37.5b
Cloud gross profit	~16.3b
Operating profit	~€11.5b
Share of more predictable revenue	approx. 86%
Free cash flow	~€7.5b

SAP's Cloud Growth

in € million @cc, continuing operations, excl. Qualtrics



- Growth drivers and new growth areas: SAP S/4HANA, SAP Business Technology Platform, SAP Signavio, SAP Taulia, SAP Business Network, SAP sustainability portfolio

Strategy

- SAP is committed to enabling every organization & every industry to become a network of intelligent, sustainable enterprises – bringing together the solutions, technology and best practices needed to run integrated, end-to-end business processes in the cloud

Market Position

Enterprise Application Software

- SAP is a market share leader in enterprise applications software, enterprise resource management applications, supply chain mgmt. applications, procurement applications software, travel and expense mgmt. software, and enterprise resource planning software acc. to IDC
- Broadest portfolio of modular and suite solutions available on premise, in the cloud and hybrid

Top Cloud Vendor

- Cloud user base: >280m users
- Cloud infrastructure: Choice across hyperscale cloud vendors (Alibaba, Amazon, Google, Microsoft) and SAP
- Largest cloud portfolio: >100 solutions for all lines of business (LoB) as well as software suites
- 248m people use SAP SuccessFactors solutions
- 55 data centers in 31 locations in 15 countries
- SAP Digital Commerce for SAP and partner online offerings >275,000 orders from >180 countries

Innovation

- R&D expense ratio: 18.9% (Non-IFRS; R&D expense as % of total revenue) for Q1/2023
- R&D headcount (FTEs): 36,150 at 3/31/2023, equaling 34.2% of total headcount
- >100 development locations worldwide
- 20 development centers worldwide (SAP Labs)
- 17 SAP Co-Innovation Labs locations worldwide
- 10 SAP Innovation Center Network locations
- >24,700 SAP partner companies in >140 countries
- Sapphire Ventures: Invested in >170 IT startups, >75 public debuts and M&As exits since 2011
  - Manages ~$10 billion in assets under mgmt.
  - Operates independently from SAP
  - Provides SAP with early access to innovations
- Support for >520 external startups
- openSAP: >1.5m unique learners, 6.6m enrollments
- Artificial intelligence: >50 live AI use cases in SAP solutions

General Facts

- Headquarters: Walldorf, Germany
- Founded: April 1, 1972
- Listing: Frankfurt, New York
- 105,132 employees worldwide (Mar. 31, 2023)
  - 157 nationalities worldwide
  - Employee retention: 93.8% (Q1/2023, rolling 12 months)
  - Employee Engagement Index at 80% (FY 2022)
  - 29.4% women in management
  - 35% women in the workplace
  - ~75% of SAP employees are SAP shareholders
- SAP has been the #1 software company in Dow Jones Sustainability Index for 16 years

Useful Links

SAP Profile – Executives – Supervisory Board – Financials – Events – SAP News Center – Photos+Films – Acquisitions – Products – Industries+Solutions – Intelligent Enterprise – Sustainability Portfolio – SAP Business Network – RISE with SAP – SAP Business Technology Platform

Portfolio

Solutions

- Packaged solutions for 26 industries and 12 lines of business: on premise, cloud, hybrid
- S/4HANA Cloud is a complete modular cloud ERP, powered by AI and analytics. It helps customers run mission-critical operations in real-time from anywhere, introduce new business models and expand globally.
- RISE with SAP: Business transformation to the cloud. Key products and services help customers drive their journey to the cloud end to end, from business process transformation to continuous innovation
- GROW with SAP: an offering optimized for mid-market customers' transformation to the cloud. It encompasses solutions, best practices, learning and adoption acceleration services
- SAP Digital Supply Chain solutions help customers achieve a resilient and sustainable supply chain, increasing productivity, improving connectivity with network collaboration, running sustainable business practices
- Spend Management:
  - SAP Ariba: connecting procurement from source to pay
  - SAP Fieldglass: >1.28 million new workers added in Q1
  - SAP Concur: >85 million end users
- SAP SuccessFactors solutions: Comprehensive and global HR software, helping organizations manage, optimize and skill their workforce. Used by >9,700 customers
- SAP Customer Experience solutions: intelligent industry solutions that help companies understand customers deeply, engage personally at scale and evolve quickly to capture new opportunities, supporting profitable growth
- >350 SAP and partner Industry Cloud solutions drive digital transformation by extending SAP S/4HANA Cloud & SAP Business Network with industry next practices
- SAP Signavio Process Transformation: process modeling, analysis and mining; governance; automated execution
- Taulia: leading working capital management solutions
- SAP Cloud for sustainable enterprises: cloud-based solutions help companies manage their carbon footprint, reduce material waste, increase social responsibility
- Services and Support portfolio provides foundational guidance, content, and learning with every cloud solution. Personalized plans and services accelerate success. Premium engagements drive large-scale change
- Localization: >660 local versions across SAP solutions

SAP Business Technology Platform (SAP BTP)

- Comprehensive and interoperable platform optimized for SAP applications, enabling application development, data management, planning and analytics, integration, automation, and artificial intelligence (AI) capabilities.
  - Intuitive, modern development environment for both IT and citizen developers (SAP Build)
  - Database, data management, analysis, and planning capabilities that maximize the value of data including SAP HANA & SAP HANA Cloud with >71,700 direct + indirect customers
  - Enterprise iPaaS and API Management to connect and automate business processes
  - AI embedded in applications to power automation, optimization, and planning and analysis
- >18,800 cloud customers are live on SAP BTP
- >1,600 partners use BTP for app development + more

SAP Business Network

- Millions of companies in 190 countries
- >$4.5tn in annual commerce
- >729m B2B transactions

Lightcast

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Expanding the Cybersecurity Talent Pipeline"

Testimony by Will Markow, Vice President of Applied Research, Lightcast

June 22, 2023

Introduction

Chairman Garbarino, Ranking Member Swalwell, and members of the Committee, on behalf of Lightcast, thank you for the opportunity to appear before you today.

As the lines between our physical and digital lives continue to blur, protecting our digital security has emerged as a defining challenge of our time. Although this challenge must be met by a mix of people, process, policy, and technology, the ultimate responsibility for our digital security rests firmly on the shoulders of our cybersecurity workforce. However, this workforce faces persistent talent challenges that choke our cyber talent pipeline and hobble efforts to build the workforce we need to secure our digital infrastructure.

It is against this backdrop that Lightcast researches and quantifies the cybersecurity workforce. We work with institutions across the public and private sectors to arm them with the data and insights they need to expand the cybersecurity talent pipeline and build a world-class cybersecurity workforce.

Lightcast is the Leading Global Authority on the Labor Market – In Cybersecurity and Beyond

Lightcast is the leading global authority on the labor market. We connect people with jobs by providing businesses, communities, and education institutions with the best labor market data and insights possible. Our data-driven insight enables better, faster decisions. To that end, we provide software products, APIs, and consulting services to employers, educators, governments, nonprofit organizations, and other institutions. We collect data from government agencies, online job postings, worker histories, and other sources from over 130 countries across the globe. Lightcast has worked with two thirds of the Fortune 100, 30 states, numerous federal agencies, hundreds of educational institutions, and dozens of nonprofits, among other clients.

Lightcast provides data and insights on all jobs and all industries, but we have been researching the cybersecurity workforce in further depth for over a decade. In 2013, we found that data about cybersecurity jobs were limited, if not missing entirely. This lack of data created an information gap that was exacerbating the cybersecurity talent gap.

Since then, we have released multiple reports on the state of the cybersecurity workforce in an effort to close this information gap. Our research has examined topics such as growth in cybersecurity hiring demand, key drivers of cybersecurity talent shortages, emerging cybersecurity skill requirements, and unique cybersecurity hiring challenges faced by the federal government, among other areas of relevant research.

The Cybersecurity Workforce Faces Two Critical Gaps: A Talent Gap and an Expectations Gap

Lightcast's research over the past 10 years has consistently pointed to a sobering conclusion: the cybersecurity talent pipeline is broken. From May 2022 through April 2023, there were over 660,000 cybersecurity job openings in the United States, but we estimate that the United States only has 69 skilled cybersecurity workers for every 100 that employers demand. This means we are stepping onto the digital battlefield missing nearly a third of our cyber army.[1] In practical terms, this means we need over 460,000 new skilled cybersecurity workers to meet employer demand.[2]

The consequences of the cybersecurity talent shortage echo across the economy. The scale and impact of cyberattacks is well known, but the consequences for companies do not end with digital breaches. Hiring costs for cybersecurity workers have skyrocketed, and cybersecurity salaries are now 10% higher than for other IT workers – despite IT already ranking among the highest-paid career fields. Cybersecurity jobs also take 21% longer to fill than other IT roles,[3] meaning many cybersecurity positions remain empty as our digital threats continue to mount.

The root causes of our broken cybersecurity talent pipeline are varied, but they can be simplified into two critical gaps: a talent gap between supply and demand of cybersecurity workers, and an expectations gap between employer demands and the realities of the cybersecurity talent pool.

The Cybersecurity Talent Gap

The talent gap between supply and demand of cybersecurity workers stem from the rapid growth and evolution in the field. Historically, cybersecurity was not a clearly delineated field and there was limited, if any, training infrastructure in place to prepare cyber workers. As a result, many workers found themselves in cybersecurity by happenstance, rather than intention. As our world became increasingly digital, however, cybercrime flourished. As a result, annual demand for cybersecurity workers has grown 200% in the past 10 years. Such rapid growth is difficult for our education system to catch up with in any field, let alone one as technically demanding and dynamic as cybersecurity.

Compounding this problem is the rapid evolution of skill requirements in cybersecurity. Cyber threats evolve daily, and the skills needed to defend against these threats must evolve as well. In just the past two years, 24% of the top skills for cybersecurity professionals have changed. Moreover, demand for emerging cybersecurity skills – especially those related to cloud security, automation, and secure application development – have grown faster than virtually any other skills that Lightcast tracks. These skills cost employers even more to fill. Just one emerging skill related to cloud security, for example, can command an annual salary premium of $15,000 or more.

In the face of such rapid skill change and inflated hiring costs, most employers struggle to keep the skills of their cybersecurity teams up to date. This struggle is even more severe for the federal government, and many federal employers lag their private sector counterparts when it comes to adopting emerging skills. Our research finds that cybersecurity teams in the private sector are 87% more likely to request

[1] Reflects the latest data from https://www.cyberseek.org/.
[2] https://lightcast.io/resources/blog/cyberseek-06-06-2023.
[3] Lightcast analysis referenced on https://www.cyberseek.org/.

emerging skills than federal employers. If the skills on our federal cybersecurity teams don't remain current, neither can our cyber defenses.

Lastly, the cybersecurity talent gap extends to cybersecurity leadership as well. Our research found that only 22% of cybersecurity managers have prior managerial experience. This means that nearly 8 in 10 cybersecurity teams are led by someone with no prior leadership experience. We also found that, on average, managers have been out of school for 11 years – more than enough time for their skills to grow stale in such a fast-moving field. This adds another dimension to cybersecurity training challenges and requires employers to invest in training for business acumen and leadership skills alongside technical mastery.[4]

The Cybersecurity Expectations Gap

The second broad cause of the broken cybersecurity talent pipeline is an expectations gap between the requirements employers demand and the realities of the cybersecurity talent pool.

In particular, many employers request inflated education and experience requirements that limit entry-level cyber opportunities. Employers request at least a bachelor's degree in 84% of cybersecurity job openings. Employers also request at least three or more years of prior work experience in, again, 84% of cybersecurity job openings.[5] Such elevated requirements are not aligned with the existing cybersecurity workforce and are rarely needed to perform the duties of a cybersecurity job. As a result, they unnecessarily constrain the pipeline of entry-level workers and limit opportunities to reach a more diverse set of candidates. They also negatively impact employee retention: in 2022, the turnover rate for cyber analysts with at least a bachelor's degree was 64% higher than the turnover rate for cyber analysts with an associate degree.[6]

Inflated certification requirements are also rampant. While certifications can be valuable signals to employers that a candidate has a certain level of knowledge, many employers have overloaded their job requirements with certifications that are unnecessary for the job for which they are hiring. This can artificially filter out otherwise qualified candidates who have the right skills, just not the right credentials.

We also have found a misalignment between the degree levels students pursue and the degree levels employers request in entry-level job opportunities. Every year in the U.S., we graduate around 3,000 fewer students from bachelor's programs in cybersecurity-related fields than there are entry-level cybersecurity jobs requesting a bachelor's degree. At the same time, we graduate over 2,900 more students from associate and master's degree programs in cybersecurity than there are entry-level openings demanding these degrees.[7] If employers reduced their degree requirements in roughly one-third of entry-level cybersecurity openings, this would nearly erase the degree-level misalignment between graduates and entry-level job opportunities.

---

[4] All data in the preceding section, "The Cybersecurity Talent Gap", reflect Lightcast analysis of proprietary Lightcast data. The data related to federal cybersecurity hiring is from Lightcast's report on the federal cybersecurity workforce, titled "Securing a Nation."

[5] Reflects Lightcast analysis of proprietary Lightcast data.

[6] Reflects Lightcast analysis of proprietary Lightcast data.

[7] Reflects Lightcast analysis of 2021 IPEDS data from the Department of Education plus proprietary Lightcast data.

This mix of talent challenges, across both the talent gap and expectations gap, has formed a perfect storm of market failures. As a result, fixing the cybersecurity talent pipeline has become a problem of remarkable complexity.

CyberSeek.org: Deciphering the Cybersecurity Job Market

Fixing the cybersecurity talent pipeline requires solutions for both the underlying talent gap and the expectations gap. To solve the talent gap, we must motivate more workers to enter the field and build the training infrastructure to support them. To solve the expectations gap, we must provide employers with the resources they need to make informed hiring decisions.

These solutions require tight coordination across employers, educators, government, students, and many other groups throughout the country. Aligning this patchwork of stakeholders is impossible without shared visibility into cybersecurity workforce needs within communities across the country.

It was this need for shared visibility that catalyzed the development of CyberSeek.org, a cybersecurity workforce analytics and career pathway platform that is freely available to the public. CyberSeek was developed in 2016 through a partnership between Lightcast, NICE, and the technology industry association CompTIA. It is funded by a grant from the National Institute for Standards and Technology. The platform provides actionable, accessible, and up-to-date information about the cybersecurity workforce in communities across the country.

CyberSeek is a unique tool that provides best-in-class data and interactive visualizations to connect the dots between employer needs and career opportunity. It includes a supply and demand heatmap, cyber career pathways, skill-based job descriptions, and a map of local training providers – all of which are completely free and open to the public. To promote additional efforts to grow the cybersecurity talent pipeline, CyberSeek also includes links to other resources on the cybersecurity workforce – including those from CISA and the National Initiative for Cybersecurity Careers and Studies.[8] CyberSeek data are aligned with the NICE Workforce Framework for Cybersecurity[9] and are updated multiple times throughout the year.

Since its release, CyberSeek has become widely used within the cybersecurity community – from students and professors to policy makers and hiring managers. Data from CyberSeek are routinely mentioned in media outlets across the country, and CyberSeek has been publicly cited by multiple presidential administrations. Many educators now develop assignments for their students to visit CyberSeek and learn more about cybersecurity careers. Inspired by the success of CyberSeek, Lightcast has helped develop two sister websites, AUCyberExplorer[10] in Australia and CyberSeek Indiana.[11] The latter is a state-level version of CyberSeek with even more localized information.

---

[8] https://niccs.cisa.gov/

[9] The NICE Cybersecurity Workforce Framework details seven key categories of cybersecurity work, as well as dozens of specialty areas and specific work roles included within each of these categories. It also includes information about the tasks performed within each work role, as well as the knowledge, skills, and abilities required to perform these tasks.

[10] https://www.aucyberexplorer.com.au/

[11] https://www.cyberseekin.org/

We are continuously soliciting feedback on CyberSeek, and we hope to continue to improve the platform so we may arm stakeholders across the country with the tools and data they need to build a world-class cybersecurity workforce.

Lightcast Supports Stakeholders Across the Cybersecurity Community

In addition to CyberSeek, Lightcast works directly with employers, educators, government agencies, and other stakeholders across the cybersecurity community. We provide best-in-class labor market data and insights through software, APIs, and consulting services. To the best of our knowledge, we are the only organization that has mapped external worker supply and employer demand data to the NICE Framework at scale.

Educators use Lightcast tools and data to inform cybersecurity program development and align their curricula with the skills that employers demand. This helps educators keep their cybersecurity programs current, and ensures their students graduate with the skills they need to secure a job. Similarly, Lightcast works with many cybersecurity certification providers to help them align their credentials with employer needs. By linking credentials with in-demand skills, we help these certifying organizations develop credentials that hold value in the eyes of both workers and employers.

Lightcast also works with employers to inform their talent decisions related to strategic workforce planning, talent acquisition, employee training, and more. We help organizations implement a skills-based approach to cybersecurity hiring, which can help expand the talent pipeline, increase candidate diversity, and improve hiring outcomes. For example, we have found that organizations taking a skills-based approach to hiring entry-level cybersecurity workers, rather than a degree-based approach, can save an average of over $15,000 per hire and expand their skilled candidate pool by over 60%.[12]

Lastly, Lightcast also works with government agencies – both at the federal level and the state, local, and tribal level – to support cybersecurity workforce development. At the federal level, we have worked with multiple departments and agencies beyond our work with NIST and NICE. In particular, we have provided information and data to the Office of the National Cyber Director and the Cybersecurity and Infrastructure Security Agency. We have also shared research findings and data on multiple interagency webinars, in meetings with federally convened working groups, and in discussions with individuals across federal agencies.

The Federal Government Can Strengthen the Cybersecurity Talent Pipeline Through Three Broad Levers: Information, Incentives, and Standards

Lightcast's work with stakeholders across the cybersecurity ecosystem gives us a unique vantage point on opportunities for the federal government to help strengthen the cybersecurity talent pipeline. In our view, there are three broad levers that Congress, CISA, and other federal actors have at their disposal: information, incentives, and standards.

[12] Reflects Lightcast analysis of proprietary Lightcast data.

Lever 1: Information

The federal government – and CISA in particular – are in a unique position to provide actionable information for stakeholders across the cybersecurity workforce ecosystem. There are multiple avenues through which this can be accomplished, but key opportunities include the following:

- **Become an exemplar for innovative, skills-based cybersecurity hiring practices.** This means shifting to a skills-based approach to hiring for cybersecurity roles and cataloging and promoting best practices for the private sector to emulate. Examples of skills-based best practices that CISA and other federal agencies can take include the following:

    - ***Reduce education, experience, and certification requirements in job openings.*** This can have dramatic impact toward reducing hiring difficulty and expanding the size and diversity of the government's candidate pool. For example, Lightcast data show that removing a bachelor's degree from early-career cybersecurity job postings can reduce the average cost to hire by over $15,000 and increase the candidate pool by over 60%.[13]

    - ***Prioritize training for high-growth, high-value skills.*** Lightcast projects that demand for many emerging cybersecurity skills will grow 50% or more in the coming years, and many of these skills command salary premiums of $10,000 or more.[14] In most cases, these skills cost considerably less to train. Focusing training on these high-growth, high-value skills – such as cloud security, DevSecOps, and others – can help the federal government maximize the return on its training investments.

    - ***Build career pathways to enhance career advancement potential for cybersecurity workers.*** CISA and other federal agencies may develop clear cybersecurity career pathways that communicate the roles that individuals may target at different stages in their careers, possible transition opportunities between each role, and the skills or other attributes workers can develop to progress between roles within a career pathway.

- **Educate employers as well as practitioners.** In addition to providing education materials for practitioners and managers, CISA or other federal actors may provide training resources for employers that outline talent management best practices for cybersecurity workers. Providing quality training resources that are accessible and targeted to personas on both sides of the hiring process can help address the dual talent and expectation gaps plaguing the cybersecurity workforce.

- **Expand and enhance access to tools and resources that support cybersecurity workforce development and hiring.** This could include the development of new tools and resources or the expansion of existing tools – such as CyberSeek, current resources from CISA and NICE, or others. These may be accomplished through either of two vehicles: increasing funding or increasing awareness.

[13] Reflects Lightcast analysis of proprietary Lightcast data.
[14] Reflects Lightcast analysis of proprietary Lightcast data.

- ***Increasing Funding:*** First, additional federal funding directed internally towards CISA or other federal agencies, or externally through grants or other mechanisms, would enable the development of new tools, functionality, and resources. For example, this may include tools providing more data on emerging cybersecurity skills, resources for employers to easily adopt skills-based hiring best practices, or even tools that directly connect individuals to open jobs or relevant training opportunities.

- ***Increasing Awareness:*** Second, expanding knowledge and promotion of existing resources can maximize their impact and help reach a larger pool of users without requiring much, if any, additional investment. For example, resources could be developed by CISA or others that provide additional "how to" guidance and case studies that demonstrate how to use existing tools and implement best practices – such as skills-based hiring. Various federal actors can also aid in the promotion of existing resources through public announcements, webinars, speaking engagements, op-eds, or other activities.

Lever 2: Incentives

The federal government is also in a singular position to influence incentives for individuals, educators, employers, and other stakeholders to help strengthen the cybersecurity talent pipeline.

For employers, this could take the form of incentivizing employer-sponsored training to upskill and reskill existing employees. These incentives may take the form of tax credits or stipends which can partially or fully offset the costs of training employees. This could improve the economics for employers to invest in training. This, in turn, may help employers strengthen the skills of existing workers and reduce the cost of hiring entry-level workers to upskill. Numerous states have developed similar programs, and the state-level experimentation and outcomes associated with these types of programs may inform similar federal programs.

The federal government may also incentivize private employers to invest in hiring entry-level workers through public/private partnerships, talent sharing, or related initiatives. This may take multiple forms, but some examples include the following:

- **Expanding shared training resources between CISA or other federal agencies and private employers.** This could reduce the cost to employers to train entry-level workers. Ideally these resources would be focused on high-value, high-growth skills – such as cloud security, DevSecOps, secure application development, and others.

- **Providing funding to local communities to support grassroots innovation.** Providing funding to state and local governments, or directly to other local institutions or consortia, can support local collaboration between employers, educators, and other local workforce development stakeholders working to grow the cybersecurity workforce. An existing example of this is the RAMPS program from NICE.[15]

[15] https://www.nist.gov/system/files/documents/2017/08/18/ramps_one_pager_032017.pdf8u_tpo.pdf

- **Providing resources, tax credits, or other financial incentives to employers to develop cybersecurity apprenticeship programs.** These programs can help students build on-the-job experience and develop diverse talent pipelines for employers. Improving the economics of apprenticeships can help more employers adopt them for entry-level cybersecurity roles.

- **Developing public/private talent sharing programs.** Under these programs, a worker can spend time working in both the public and private sector, which helps them gain new skills and on-the-job experience. CISA has already experimented with similar programs on a limited scale. These talent sharing programs could support greater information and resource sharing between the public and private sector and would help workers in all sectors build new skills. It may also reduce hesitancy for employers to hire entry-level workers if they are able to share the training of those workers with federal employers.

Lever 3: Standards

Lastly, the federal government can develop standards and frameworks that support consistent application of best practices related to workforce development, training, and hiring. Already, NIST and NICE are providing valuable standards and frameworks related to cybersecurity. This also extends to cybersecurity education and workforce development, which is most prominently achieved through the NICE Framework.

The NICE Framework has become a valuable resource that is used widely in the cybersecurity community. Educators use the NICE Framework to inform their training content and align it to the needs of the workforce, employers use it to assess gaps in their cybersecurity workforce, and individuals use it to identify the types of work they can prepare for within the cybersecurity field, among other stakeholders.

Building off the success of the NICE Framework, the federal government may take additional steps to provide standards and frameworks that will strengthen the cybersecurity talent pipeline. Some of these steps may include the following:

- **Provide frameworks and standards that outline best practices for cybersecurity employers.** This may include standards describing best practices for adopting skills-based hiring, optimizing job descriptions, building career pathways, maximizing the value of learning and development, developing apprenticeships, engaging with educators or other stakeholders, and related activities. This will help to address the expectations gap that creates misalignment between the needs of employers and the realities of the existing cybersecurity talent pool.
- **Continue to update and refine the NICE Framework.** The rapid evolution of cybersecurity skill requirements necessitates frequent updates to the NICE Framework to ensure it remains current. Moreover, additional data collection and industry input can help NICE continue to further align the Framework with the language and needs of employers.
- **Provide frameworks and standards for educators to build training content that is up-to-date and aligned with employer needs.** This may take the form of baseline standards for curriculum development, suggested steps for data collection and analysis on market job and skill demand, recommendations for strengthening employer engagement, tools for embedding hands-on

learning opportunities into curricula, resources for developing co-ops and internship opportunities with local employers, and related activities.

Conclusion

Expanding the cybersecurity talent pipeline is, undoubtedly, a complex issue. It requires coordination across a constellation of disconnected, yet interrelated, educational institutions, employers, and individuals. Aligning this diverse ecosystem of stakeholders requires a shared understanding of the problem, and clear, level-headed guidance on how to solve it.

Thousands of stakeholders – both in the public and private sectors – are already facing this challenge head on. Lightcast is committed to working with these stakeholders, and we welcome collaboration with anyone interested in creative, data-backed solutions to cybersecurity's pipeline challenges.

Thank you again for the opportunity to participate in this hearing an I look forward to further engagement with the Committee.

Respectfully,

William Markow

Will Markow
Vice President of Applied Research
Lightcast

TESTIMONY OF

Colonel Chris Starling (Retired)
Executive Director, NPower California

BEFORE

Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection

ON

"Growing the National Cybersecurity Talent Pipeline"

June 22, 2023

Chairman Garbarino and Ranking Member Swalwell, distinguished members of the Committee—thank you for the privilege to appear before you today on behalf of NPower to discuss growing our national cybersecurity workforce talent pipeline.

My name is Chris Starling, I am a retired colonel of the U.S. Marine Corp, where I served for over 26 years. Since 2019, I joined NPower to run our program in the Bay Area.

NPower is the premiere technology training organization providing young adults, veterans, and Women of Color from underrepresented communities with free tech training, social and emotional support, and full-time job placement assistance with many of the nation's leading employers. Annually, we serve over 1,300 unemployed and underemployed students across the country with high-quality tech workforce training leading to industry certification, with social support, professional development, and job placement services.

We work at the intersection of poverty alleviation, equity, workforce diversity and the tech industry. Our program is delivered free of charge to men and women earning less than 200 percent of the federal poverty level, and they primarily come from racial and socioeconomic backgrounds underrepresented in the tech industry.

Technology is one of the main drivers of the US economy, and the demand for talent constantly outpaces the supply of skilled workers. Experts project tech sector employment to grow at the fastest rate of all occupations – and people simply aren't entering the field fast enough to replace retiring workers. Various factors are driving the increase, from innovations to natural disasters to the Covid pandemic, which prompted the whole country to work and deliver services remotely.

In addition to the shortage of skilled talent, there's an enduring lack of diversity in the IT workforce that has long been recognized as a systemic national problem. Many tech job seekers today lack college degrees and therefore are overlooked in the talent sourcing of many companies. NPower meets

learners where they are and offers them industry-recognized certifications and certificates to demonstrate their skill over pedigree.

At NPower, we believe access to high-growth careers is possible for anyone, no matter where you start. We believe this is our key to creating a world where equity is possible. We blend best-in-class and trauma-informed tech training and personal support, to constantly innovate new ways to foster talent. A specialized team of Social Support Managers provide 360-degree support services by connecting our students with city and social service agencies for all their social and emotional needs.

With our approach, we're building a new kind of pipeline to tech careers. Our students don't come from traditional backgrounds and many of them come to us at a pivotal moment of transition in their lives. We don't see that as a hindrance: we recognize their worth as powerful assets in their local communities. With our comprehensive support, they can leverage their own internal hunger, grit, and determination to drive change in their personal and professional lives.

NPower's Key Workforce Performance Metrics

NPower has trained 560 individuals from under-resourced communities in cybersecurity since 2015.

NPower evaluates impact based on program completion, attainment of industry credentials, and placement in quality jobs or continuing education. Our Key Performance Metrics map directly to the Workforce Innovation and Opportunity Act (WIOA) performance metrics used by most workforce development programs. Below are our impact metrics for our cybersecurity program:

- 85 percent of enrolled students complete training on time and graduate
- 88 percent of graduates secure at least one industry-recognized credential
- 81 percent of graduates are placed in quality employment or enrolled in continuing education at six months and one year after graduation

We track Measurable Skills Gains through demonstrated mastery of key competencies in hands-on labs and assignments, tracked through our custom Learning Management System.

We also track income growth pre- and post-program. Consistently, at their first job post-program, NPower graduates achieve an immediate and dramatic salary increase that meets or exceeds the MIT Living Wage for their region. On average NPower graduates saw an average increase of roughly 420 percent, rising from an average pre-program income of $9,374 to an average post-program salary of $43,260. For our cybersecurity graduates their post-program wage average is $63,372! Their wages continue to grow as they gain experience, and the positions for which we train are designated by the U.S. Department of Labor as "Launchpad Occupations" with higher-than-average salary growth. Our team continues to reach out to alumni periodically after the initial job placement to support and track job retention, promotions, raises, and overall career trajectory.

Cybersecurity Infrastructure and Security Agency (CISA) NPower Grant:

In 2021, CISA awarded NPower a $1 million grant for the development of cyber workforce training. The partnership focuses on the development of a scalable and repeatable proof of concept to identify and train talented individuals around the country and help address the staggering cybersecurity workforce

shortage facing our nation, while also meeting the dynamic needs of the cybersecurity workplace. CISA supports non-traditional job training and apprenticeship programs like NPower and acknowledges that more readied talent could lead federal government, state, local, tribal and territorial entities, as well as private sector employers to address current and future cyber workforce needs.

The program has been successful thus far:

- Fall 2021
    - 91% job placement
- Spring 2022
    - 100% retention
    - 100% certification
    - 72% job placement
- Fall 2022 (mixed TF & Cyber)
    - 100% retention
    - 82% certification
    - 77% placement
- Spring 2023: Week 16
    - 100% retention
    - 50% certification
        - Certification is in progress

Policy Recommendations

We would like to offer to the committee the following policy recommendations as you seek to address the cybersecurity workforce shortages:

1. Establish a permanent program that includes the core principles of the pilot program on which CISA is currently collaborating with NPower. Expanding the pool of cyber talent requires sustainable and adequate funding.

    Core Principles of the Program are:

    - Partner with nonprofits and government agencies to upskill men and women from underserved communities;
    - Invest in credential-focused short-duration cybersecurity workforce training programs that enable them to earn while learning;
    - Provide professional and soft skills development training alongside technical skills training;
    - Provide wraparound social support to ensure basic needs for housing, food and childcare, eliminating the barriers to success;
    - Provide job placement support and ensure they gain crucial paid work experience;
    - Engage and incentivize employers to shift hiring practices to focus more on skills-based hiring, nontraditional talent and apprenticeships;
    - Create direct talent pipelines from training programs to employers;

- Support long-term career pathways with plenty of training on-ramps and off-ramps, recognizing it may take individual workers years of entry-level tech training, alternating with work, and continuing education to attain a journeyman's level of cybersecurity expertise.

2. Invest in Platforms for On-Demand Help Desk support for individuals, nonprofits and small businesses. NPower is spearheading a national network of Community Help Desks that provide free technical assistance and digital navigation to local underserved communities, staffed by graduates of our tech workforce training programs gaining vital work experience as Registered Apprentices. NPower's programs are aligned to national standards for U.S. Dept. of Labor Registered Apprenticeship Programs.
    - Community Help Desks provide critical human support to help people on the wrong side of the Digital Divide take advantage of online job, health and education resources, while offering trainees the opportunity to build their resume through a paid apprenticeship.
    - The Community Help Desk will serve as an especially vital resource to local underserved seniors, public school families, adult learners, and jobseekers. The model capitalizes on partnerships with community-based organizations, and can provide a central hub for affordable connectivity and device distribution.

3. Modernize and reform Federal workforce hiring practices to adopt skill-based hiring practices and the Registered Apprenticeship model for technical roles. This allows the Federal government to compete for a talented and diverse workforce pool that prioritizes skills and a candidate's ability to do the job, and leads by example in equity-focused workforce development

4. Establish a grant program within the Department of Labor to support the creation, implementation, and the expansion of registered apprenticeships in Cybersecurity and Information Technology, modelled on high growth state apprenticeship programs such as California, Texas and Michigan. Specifically, the Secretary of Labor should provide grants, on a competitive basis, to support the establishment, implementation, and expansion of registered apprenticeship programs in cybersecurity and technology.

5. Integrate relevant state and federal policy issues into cybersecurity workforce training programs. A growing contingent of cybersecurity job openings require both technical and legal knowledge to guide companies on issues of privacy and security.

6. Capitalize on the promising talent pool of military-connected individuals and families, including transitioning Military Servicemembers, Veterans, Reservists, National Guard, and their often-overlooked spouses. Department of Defense statistics show 80% of military leave service without another job in place. The protective nature of military service leaves them well-suited for a cybersecurity career, and many already carry higher-level security clearances from their military years. They are a diverse group, with a majority who come from racially and socioeconomically marginalized populations. Military-connected individuals offer an especially promising talent pool from which to grow a strong, diverse cybersecurity workforce.

Conclusion

To address our cybersecurity workforce, we must find innovative ways to grow our workforce talent pool. For us, a key component has been embedding cybersecurity skills, concepts, and competencies throughout our expanded learning pathways. In addition, we seek to provide security awareness support services and troubleshooting to underrepresented communities as part of our national community help desk.

We believe the key to unpacking this unlimited potential and talent comes from building training and support programs to command a shift by partnering with government, industry, and employer partners in recruiting, hiring, assessing skills and competencies, and supporting people into cyber tech careers from various learning pathway.

Thank you for the opportunity to appear before you today and I look forward to taking your questions.

ISC2
625 N Washington Street, Suite 400
Alexandria, VA 22314
ISC2.org

House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection Hearing on "Growing the National Cybersecurity Talent Pipeline"
June 22, 2023

Written Testimony of Tara Wisniewski
Executive Vice President for Advocacy, Global Markets, and Member Engagement
ISC2

ISC2 thanks Chairman Garbarino and Ranking Member Swalwell and the members of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection for the invitation to testify at this important hearing on the national cybersecurity talent pipeline. We appreciate the opportunity to share our perspective on the current state of the cybersecurity workforce and our vision for the future. The Cybersecurity and Infrastructure Security Agency (CISA) has been a critical partner in the work to close the cybersecurity workforce gap, among the many other roles it plays in securing cyberspace. In particular, we greatly appreciate CISA's role in creating a safer and more secure cyber ecosystem through the harmonization of standards and regulations, encouraging collaboration between public and private entities to defend critical systems and information, investing in a cyber resilient future for public and private sector stakeholders, and defending against an ever-evolving threat landscape.

ISC2 is a Leader in Developing the Global Cybersecurity Workforce

ISC2 is an international nonprofit membership association focused on building a safe and secure cyber world. Our organization is dedicated to understanding and addressing the barriers facing the cybersecurity workforce and serving as a leader in the implementation of solutions that will build and support a well-qualified and diverse workforce in the United States and globally.

Best known for our acclaimed Certified Information Systems Security Professional, or CISSP®, certification, ISC2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association is made up of over 425,000 members, associates and candidates across the globe, including approximately 200,000 in the United States. Our members are a critical part of delivering on our mission, given the tremendous work they engage in daily to advance the industry and ensure we live in a more secure world. Our membership includes a variety of certified cyber, information, software, and infrastructure security professionals responsible for securing our governments, economies, critical infrastructure, and personal information every day.

Our charitable foundation, the Center for Cyber Safety and Education, supports ISC2's vision for expanding the cyber workforce and enhancing cybersecurity by educating the public about cyber risks, removing barriers to accessing the cybersecurity profession, and helping small organizations protect themselves from cyber risks.

The State of the Cybersecurity Workforce

With geopolitical and macroeconomic turbulence, a constant flood of high-profile cyberattacks threatening critical infrastructure and business resilience, and an evolving regulatory environment driving new cyber governance and compliance requirements, the stakes have never been higher. Mission critical to all of these concerns is the need for a well-rounded, skilled cybersecurity workforce.

Understanding the gravity of the demand for cyber talent as threats expand and organizations become increasingly aware of the vital importance of resilient cyber systems is essential for building solutions. This need for accurate data drives ISC2 to conduct our annual Cybersecurity Workforce Study to assess the size of the current cybersecurity workforce, as well as the existing talent shortage. This research has given us tremendous insight into the challenges and opportunities cyber professionals face, including hiring and recruiting trends, corporate culture and job satisfaction, career pathways, certifications, professional development, how the workforce is adapting to current events, and what the future of cybersecurity work looks like. It also shows us what conditions are essential to shrinking the talent gap.

Our 2022 Cybersecurity Workforce Study found there to be global unfilled demand, or a workforce gap, of 3.4 million cybersecurity workers, representing a 26.2 percent year-over-year increase. In the U.S. specifically, our cybersecurity workforce grew by 5.5 percent, reaching a total of 1.2 million cyber professionals in 2022. But at the same time, the estimated workforce gap grew 9 percent last year as more organizations realized their need for cybersecurity professionals and additional cyber roles opened up. In the U.S. in 2022, we estimate the cyber workforce gap is around 410,695 unfilled roles.[1]

Given these numbers, the lack of a qualified cybersecurity workforce continues to be a top concern for all sectors, particularly critical infrastructure. 72 percent of U.S. respondents reported their organization does not have enough cybersecurity employees, and 55 percent of those respondents said these staff deficits put their organization at a "moderate" or "extreme" risk of a cyberattack.[2] As our world becomes more digitally reliant, the potential for cyberattacks grows and businesses and data must be protected. In fact, 95 percent of small businesses are unprotected, highlighting the critical need to ensure organizations of all sizes are able to find and retain qualified cybersecurity talent.[3]

ISC2 is currently in the process of analyzing data for our 2023 Cybersecurity Workforce Study, which will be released in September 2023. Early estimations show there are 132,000 new entrants in the U.S. cybersecurity workforce, an 11 percent increase from last year's numbers, while the workforce gap grew to 482,985 unfilled roles.

---

[1] ISC2 2022 Cybersecurity Workforce Study. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[2] Ibid.
[3] Ibid.

ISC2 Efforts to Build a Qualified and Diverse Workforce

Considering these staggering cybersecurity workforce statistics, ISC2 is committed to finding solutions to address the cybersecurity workforce gap in the United States and around the world. Since our founding, ISC2 has been a leader in credentialing the global cybersecurity workforce with standards-based approaches to skills development. This is reflected in the Common Body of Knowledge for all ISC2 certifications and training materials, as well as our commitment to mapping all of our certifications to international standards. Further, our ecosystem of education and certification is built on a solid foundation of ethical best practices to which all members must adhere. For a profession that is critical to every major sector, expanding access to the cybersecurity profession, as well as setting reasonable, concise and effective standards that include certification requirements, is pivotal.

Over the last several years, ISC2 has increased our focus on the full lifecycle of the cybersecurity workforce, and we continue to serve as an advocate for the profession and the professionals we serve. As part of this work, we are committed to creating a diverse talent pipeline through education, upskilling, re-skilling, and professional development. We have a particular focus on developing and supporting entry-level and early career professionals to ensure we have more entrants into the profession – where they are most desperately needed – to help meet the ever-widening gap.

One of the most critical investments we made last year was the development of an entry-level certification called the ISC2 Certified in Cybersecurity (CC). This certification allows those with little to no cybersecurity experience to gain the foundational knowledge, skills, and abilities necessary for an entry-level cybersecurity role. The CC certification is ideal for current IT professionals or other professionals looking to transition into cybersecurity, as well as college students or recent high school graduates interested in exploring the cybersecurity field. We believe this certification fills a critical gap in the cybersecurity workforce by providing an on-ramp for potential cybersecurity professionals to begin their careers and launch into their first jobs where they can continue to learn, grow, and access other certifications along their career path.

In light of our pledge to implement meaningful solutions to the global workforce cybersecurity workforce challenges, ISC2 not only created the CC certification, but we also have pledged to deliver One Million Certified in Cybersecurity courses and exams — for free.[4] We made this commitment during the Cyber Workforce and Education Summit at the White House last summer and are pleased to report that over 23,000 professionals have earned the CC certification since that time, and more than 200,000 have enrolled in the program. As part of this commitment, we also pledged to direct half of these course enrollments and exams to students of historically black colleges and universities (HBCUs), minority-serving institutions (MSIs), tribal organizations, and women's organizations.

[4] ISC2 Pledges One Million Free ISC2 Certified in Cybersecurity Courses and Exams. https://blog.isc2.org/isc2_blog/2022/07/isc2-1-million-certified-in-cybersecurity.html

U.S. Federal Government Solutions to Address the Workforce Gap

Protecting the nation's critical infrastructure has never been more important as our forthcoming 2023 workforce study will show that more than half of information security professionals currently in those sectors believe their organizations are at a moderate to extreme risk of experiencing a cybersecurity attack. When hiring for cybersecurity positions, hiring managers put cybersecurity certifications at the top of list of qualifications they find most important. According to our data to be released in the coming months, among the skills hiring managers are looking for, risk assessment, analysis and management were at the top of the list (31 percent), while communications skills (29 percent); security engineering (28 percent); and governance, risk management and compliance (27 percent) were also listed as important. When considering the needs of securing our critical infrastructure, ISC2 research suggests hiring managers in those sectors are open to nontraditional methods of increasing the workforce including prioritizing nontechnical skills and providing training and development for employees once hired.

ISC2 is extremely proud of the work we have done to date to help address the gaps in the cybersecurity talent pipeline, but we recognize we cannot do this work alone. Governmental bodies around the world, including the U.S. federal government, will play an important role in creating policy and regulatory environments that allow cybersecurity professionals to thrive and grow. Given its mandate from Congress, the Department of Homeland Security and CISA specifically will be important stakeholders in finding and implementing solutions to address the current workforce gap we experience in the United States.

We commend the Biden Administration for its work on the 2023 National Cybersecurity Strategy, particularly the strategy's focus on enhancing the cybersecurity workforce, increasing coordination and collaboration in public-private partnerships, responding to threats on critical infrastructure, and clarifying the responsibility of various entities in the cyber ecosystem for responding to cybersecurity threats.

We believe efforts to create a strong and secure national and global cyber ecosystem built on partnership, communication, responsible action, and technological development are critical to addressing vulnerabilities throughout the public and private sector. We look forward to seeing the Administration's forthcoming cyber workforce strategy, which will provide even more specificity to the federal government's plans to utilize its current authorities, structures, and programs to continue to develop the cyber workforce throughout the country.

To ensure the success of the National Cybersecurity Strategy, all federal agencies, including CISA, will play a critical role in its implementation. CISA's strengths in the implementation will stem from its role in raising awareness and increasing the visibility of cybersecurity and the important role cyber defense plays in protecting against the growing threats facing the nation. The agency should continue to play an instrumental role in promoting dialogue and building knowledge and awareness of information and systems security across the digital landscape. It also is important for CISA to continue to serve as a conduit between government agencies and the private sector to encourage collaboration, increase diversity within the sector, and explore and implement other measures related to cyber readiness to effectively manage the increasing cybersecurity risks facing the U.S.

To be clear, none of the goals in the National Cybersecurity Strategy can be accomplished without focusing on the need for more cybersecurity professionals and professionalizing the cyber sector to ensure cybersecurity professionals are equipped to respond to evolving threats. To address these issues, the U.S. government and industry need innovative strategies for workforce development as the strategies of the past have not been sufficient to address the prolific cybersecurity workforce crisis. The answer to the cybersecurity workforce problem will not be found in a single program but rather a multitude of innovative solutions, including the recommendations outlined below.

- **Provide pathways for entry-level practitioners to join the cybersecurity field.** ISC2 conducted a recent study of hiring managers to learn more about the best practices for hiring and developing entry-level cybersecurity practitioners. Our research found that organizations focused on recruiting and developing entry-level cybersecurity staff, including those with little or no technical experience, are helping to accelerate the invaluable hands-on training that the next generation of professionals need.[5] Yet, it is often difficult for professionals to get their foot in the door into those initial roles to gain access to this valuable experience.

  Understanding that what employers need most to shore up their cyber defenses is entry and junior-level cybersecurity professionals – degrees are not necessarily required for valuable early-career roles – ISC2 developed the CC certification to address this problem. Yet, there is more to be done to open the floodgates for these pathways into the cybersecurity profession. Organizations and the government must be willing to step in to provide incentives and hire entry-level professionals with entry-level qualifications, as well as invest in the professional development of these professionals – otherwise, we will never create the talent pipeline necessary to bridge the workforce gap.

  We are encouraged by several of CISA's education and career development programs, including the Cybersecurity Education and Training Assistance Program (CETAP) to inspire the next generation of cybersecurity professionals through initiatives to include cybersecurity education in K-12 schools. We also appreciate CISA's work on the Cybersecurity Workforce Development and Training for Underserved Communities program, which is designed to increase diversity across the cyber workforce, as well as the Cyber Career Pathways Tool to help people gain a better understanding of cybersecurity and the different roles available in the sector.

- **Increase diversity within the cybersecurity field.** Given the wide range of threats we see in the cybersecurity realm, it is imperative we consider how to diversify the cybersecurity workforce to ensure we have a diversity of thought and experience available leading our cyber defenses. One of our recent market research studies found that incentivizing a more diverse information and systems security profession

[5] ISC2 Cybersecurity Hiring Managers Guide. https://www.isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ashx

encourages increased innovation.[6] For example, our study showed organizations with diverse leadership teams benefit organizations culturally as well as in their bottom-line revenues.[7] This diversity also adds to the overall confidence of an organization's security posture given that highly diverse teams can directly contribute to greater success and prosperity. Yet, despite these findings, meaningful progress to deliver greater and more equitable diversity and inclusivity within the cybersecurity profession has been slow.

CISA can help in these efforts to diversify the cybersecurity profession by channeling education resources to redefine the image of the cybersecurity professional and the profession to accurately reflect and value the diversity of the world it protects. We hope to work with CISA to find innovative ways to continue to bring people into the sector and retain them because we recognize that we must focus our efforts not only at the entry- and mid-levels but at the C-suite and executive levels as well. To create a diverse and inclusive workforce and reap the resulting benefits, diversity must be prevalent at all levels of the organization.

- **Facilitate collaboration with private sector entities.** Collaboration is key to addressing cybersecurity vulnerabilities and the workforce gap. As a global organization with strong connections to lawmaking bodies and government entities across the world, ISC2 recognizes the importance of continuing to build strong partnerships and strengthen collaborative relationships to further the profession's needs.

  CISA's commitment to sustain long-term dedication to the sector provides us with a natural partnership in this area. Working together, we can provide more cybersecurity readiness resources across all levels and roles in the public and private sector for the information and systems security profession.

  We believe it is important to consider the federal government's role in addressing the cyber workforce gap, while acknowledging the private sector's existing efforts to find creative solutions to this problem. Working together, we believe there are many opportunities to increase education, incentivize professional development, and develop programs that are available to as many people from as many backgrounds and demographics as possible.

- **Professionalize cybersecurity.** A digitally skilled population and strong cybersecurity workforce leads to more resilient organizations and infrastructure. This is especially important as the United States seeks to create more and better paying jobs, spur prosperity, increase diversity and drive economic growth across the nation. Given the nascency of the cybersecurity profession, it is critical to consider how we can continue to professionalize cybersecurity to ensure there is a clear and understandable career path for professionals interested in joining the field.

[6] ISC2 "In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity." https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx
[7] Ibid.

The professionalization of other sectors such as finance and accounting, which spans more than a century, is a model for the cybersecurity field to follow as we look for ways to set standards, establish ethical expectations and increase public trust in our cybersecurity professionals. Certifications are a critical part of this work, including ensuring cybersecurity professionals hold certifications accredited by international standards bodies. Additionally, the profession will continue to benefit from ongoing professional education, immersive courses, and other professional development opportunities, including determining ways to upskill within an organization to fill outstanding cybersecurity roles.

Thank you for the opportunity to testify before the subcommittee and provide input on this important topic. ISC2 greatly appreciates your interest in this issue and your willingness to explore ways the federal government can work together with stakeholders in the cybersecurity space to address the gaps we are seeing in the cybersecurity workforce. We look forward to continuing to work with the subcommittee to find solutions that will benefit cybersecurity professionals, the organizations they serve, and the public overall.